PRÍBEH 1>

# SKUTOČNÝ ÚTOK NA SLOVENSKÉHO AUTOMOTIVE DODÁVATEĽA — KROK ZA KROKOM.

GALANTECH

# DODÁVATEĽ PLASTOVÝCH KOMPONENTOV PRE AUTOMOTIVE.

PROFIL FIRMY

| 180 | 2,5M€ | Tier 2 | DE · CZ |
|---|---|---|---|
| zamestnancov | ročný obrat | dodávateľ v automotive reťazci | nemecké a české automobilky ako odberatelia |

Faktúry chodia mailom.
Objednávky chodia mailom.
Firma má antivírus, firewall aj zálohovanie
— **má všetko, čo má bežná SK firma.**

JEDEN JÚLOVÝ DEŇ

# TELEFONÁT, KTORÝ NEDÁVAL ZMYSEL.

| | |
|---|---|
| PLASTMETAL | **„Ste 14 dní po splatnosti.“** |
| GALANTECH | Posiela potvrdenie o úhrade. Zdá sa, že všetko je v poriadku. |

## + 7 DNÍ:

| | |
|---|---|
| PLASTMETAL → ŠÉFOVI | **„Zastavujeme dodávky tovaru. Úhrada stále neprišla.“** |
| ŠÉF GALANTECH | **„Všetko je urovnané, pošlem vám potvrdenia znova.“** |
| PLASTMETAL CFO | **„Máte problém. Toto potvrdenie nesedí s tým spred týždňa — a je na ňom cudzie číslo účtu. My máme stále to isté.“** |

ČO SA NAOZAJ STALO

# EMAIL OD ZNÁMEJ OSOBY — KTORÝ NEBOL OD NEJ.

Prišlo oficiálne oznámenie o zmene čísla účtu.

Od pani z finančného oddelenia PLASTMETAL, s ktorou GALANTECH bežne komunikuje.

Adresát: hlavná účtovníčka, pani Adamová.

Pár dní pred ďalšou fakturáciou — presné načasovanie.

Žiadne podozrenie — sedel jazyk, štýl aj formát.

Potvrdila zmenu emailom a prepísala číslo účtu v účtovnom systéme.

Ďalšia faktúra bola úplne korektná.

Sedeli množstvá, počty aj sumy. A obsahovala nové číslo účtu.

JADRO PODVODU

**Všetko sedelo. Iba peniaze odišli na účet útočníka.**

Dodávateľ za úhradu aj „poďakoval“ emailom — falošným.

TRI MESIACE TICHA PRED DŇOM D

# JEDEN KLIK V MARCI. PLATBA ODIŠLA V LETE.

## Marec

Účtovníčka klikne na phishing imitujúci Microsoft. Heslo putuje útočníkom.

## Apríl

Útočníci čítajú schránku, mapujú kontakty a štýl komunikácie.

## Máj

Analýza splatností a interných procesov. Príprava šablón.

## Jún

Registrácia lookalike domény GALANTACH.SK

## Júl

Deň D — spustenie dvoch paralelných útokov naraz.

ČO SA STALO V EMAILOVÝCH SCHRÁNKACH

# ÚTOČNÍK NEČÍTAL LEN MAILY — PREPISOVAL ICH.

## KONTROLA NAD KOMUNIKÁCIOU

**Kompromitované schránky**: pani Adamová (účtovníčka) aj pán Novák (šéf).

Nastavené **presmerovanie**: celá komunikácia s PLASTMETAL kópiou na externú schránku útočníka.

Pravé maily sa potichu **zahadzovali.**

Namiesto nich chodili podvrhy — falošná faktúra, falošné potvrdenie o úhrade.

## DRUHÝ CIEĽ · AUTOWERK

Vyšetrovanie odhalilo paralelný útok na veľkého odberateľa.

Útočníci založili falošnú doménu a začali z nej komunikovať.
Podobný scenár — zmena čísla účtu pred platbou.
AUTOWERK zmenu nezrealizoval. Ku škode tu nakoniec nedošlo.

**Jeden prienik, dva nezávislé pokusy o podvod.**

# JEDNA KOMPROMITÁCIA. DVA PODVODY.

PRÚD 01 · SUBDODÁVATEĽ

## Falošná faktúra od subdodávateľa

Útočník zachytil faktúry od PLASTMETAL a prepísal na nich IBAN. GALANTECH zaplatil na účet útočníka.

**242 000 €**

UHRADENÉ PENIAZE NEVRÁTENÉ

PRÚD 02 · ODBERATEĽ

## Falošná zmena IBAN-u odberateľovi

Z lookalike domény poslali AUTOWERK-u žiadosť o zmenu účtu pre platby smerujúce do GALANTECH-u.

**380 000 €**

ZABRÁNENÉ ZMENU NEZREALIZOVALI

DOPADY NA GALANTECH

# STRATA 242,000 EUR. ÚČET VÝRAZNE DLHŠÍ.

01 · FINANCIE

### 242 000 €

Platba do zahraničia, prijímateľ nespolupracuje, peniaze sa nepodarilo vrátiť.

02 · PRÁVO

### Trestné oznámenie

Prípad odstúpený do zahraničia. Banka platbu nevie zvrátiť.

03 · NÁKLADY

### Forenzná analýza a právne služby

Externé tímy, audit incidentu, právne zastúpenie — všetko nad rámec straty.

04 · DÔVERA

### Subdodávateľ žiada predplatby

Narušený vzťah s dodávateľom, nové platobné podmienky v jeho prospech.

05 · ODBERATEĽ

### Bezpečnostný audit od AUTOWERK

Kľúčový odberateľ preveruje, či je s GALANTECH-om bezpečné obchodovať.

06 · ĽUDIA

### Reputácia a neistota

Účtovníčka s neistou budúcnosťou. Otázniky u partnerov aj zamestnancov.

# ČO BY SPRAVILA ODOLNÁ FIRMA INÁČ?

Expertné pohľady na ten istý prípad

01
**PREVENCIA**

02
**DETEKCIA**

03
**REAKCIA**

04
**LEGISLATÍVA**

# 01

# PREVENCIA

Technológie a procesy, ktoré útok zastavia skôr, než vôbec začne.

# 02

# DETEKCIA

# 03

# REAKCIA

03

Prvé hodiny rozhodujú.

# 04

# LEGISLATÍVA

NIS2, GDPR a zodpovednosť vedenia..

# ŠTYRI ODPORÚČANIA, ”SO SEBOU.”

**01** **DMARC v režime reject + MFA pre všetkých.** Základ, ktorý sám zastaví väčšinu lookalike a phishing mailov.

**02** **Spätné overenie pri každej zmene IBAN-u.** Iným kanálom než email a na vopred známe číslo.

**03** **Systém „štyroch očí“ pri dôležitých zmenách a transakciách.** Žiadna kritická platba ani zmena účtu na jeden podpis.

**04** **Simulované phishingy a kultúra „pýtať sa je v poriadku“.** Otázka „je to naozaj tak?“ má byť normou, nie výnimkou.

01

Ani jeden z nich nebol o geniálnom hackingu. Boli o zle nastavených nástrojoch a procesoch.

02

Rozhodli postupy a (ne)príprava — všetko spravené dávno pred incidentom.

03

Odolnosť nie je produkt. Je to spôsob, akým je firma postavená.

# Dva veľmi odlišné útoky. Rovnaký záver.